University of Sussex

IET Lecture,
Richmond AS03, Sussex Campus
21st February 2017

Classical and Quantum Optical Computing

Rupert C. D. Young, Philip M. Birch and Chris R. Chatwin

Department of Engineering and Design
University of Sussex, Brighton, UK

University of Sussex

Introduction

- Classical coherent optical processing
- Optical Fourier transform
- Two dimensional correlation – 4-*f* coherent optical correlator

University of Sussex

Introduction

- Coherent optical implementation of the Discrete Fourier transform (DFT)
- Coherent matrix-vector multiplier
- DFT as a Unitary Operation
- Fast Fourier transform (FFT) decomposition of DFT
- Coherent optical implementation based on FFT signal flow diagram

University of Sussex

Introduction

- Electro-optical implementation of the FFT ‘Butterfly’ operation
- The quantum Fourier transform (QFT)
- Similarities and differences of coherent optical FFT to the QFT
- Grover’s search algorithm implemented with a coherent optical correlator
- Quantum algorithms requiring bit entanglement - Shor’s algorithm for large number factorisation

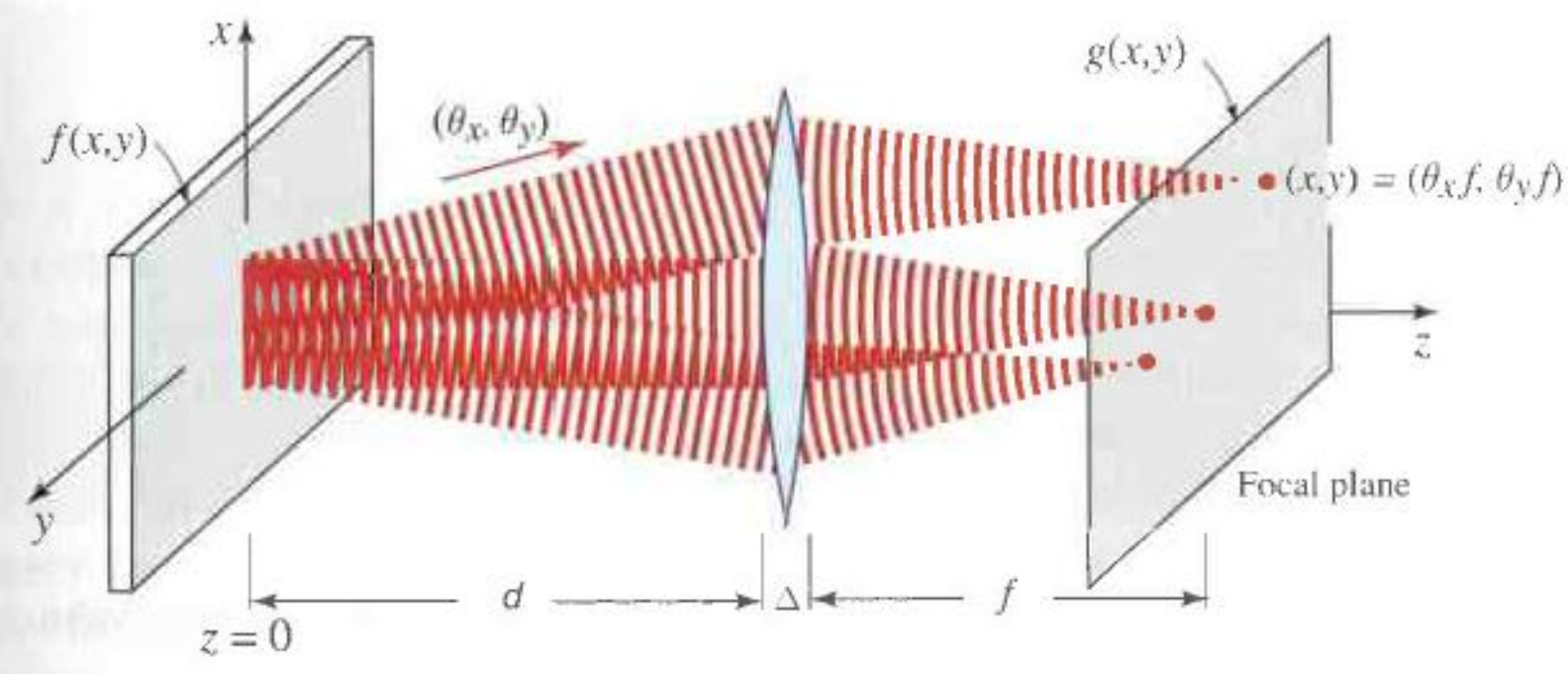
University of Sussex

Introduction

- Spatial Light Modulator (SLM) pixels placed in a binary superposition state. Addressed with an “interaction free” measurement
- Allows exponential increase in processing power
- Quantum search algorithm for a decryption problem based on superposition state of coherent wavefront
- Conclusions

University of Sussex

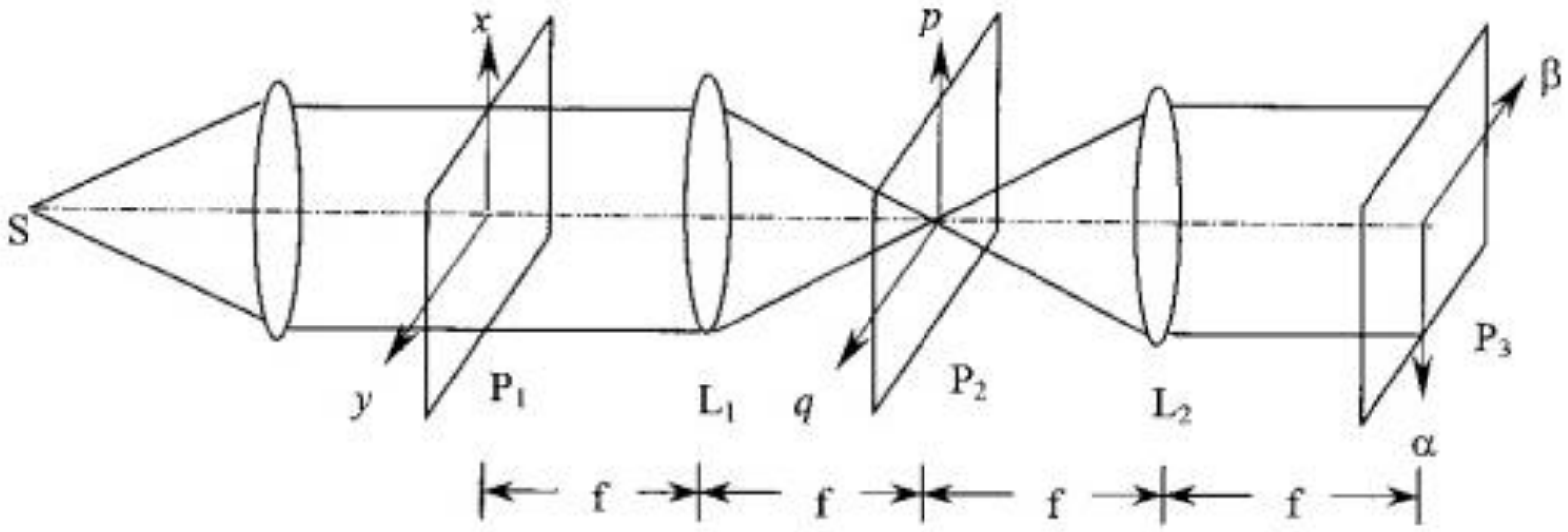
Optical Fourier transform



Saleh and Teich, Fundamentals of Photonics, Wiley

University of Sussex

Coherent optical processor – 4-*f* correlator configuration



$$z(\alpha,\beta) = F^{-1}\left(F(g(x,y))F^{*}(h(x,y))\right)$$

$$z(\alpha,\beta) = \iint_{A} g(x,y)h(x+\alpha,y+\beta)dxdy$$

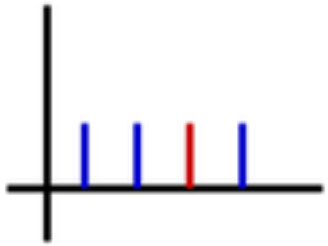
University of Sussex

The Grover data search algorithm

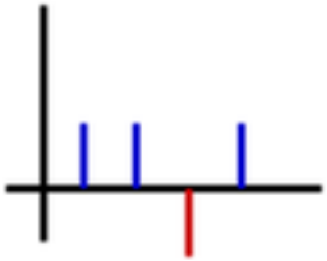
- Problem – find a data entry in an un-ordered database
- Requires $O(N/2)$ searches on average for a an *N* element database
- Grover quantum search algorithm can reduce this to $O(\sqrt{N})$
- Involves quantum interference but does not require entanglement of bits in a quantum register
- Coherent optical implementation

University of Sussex

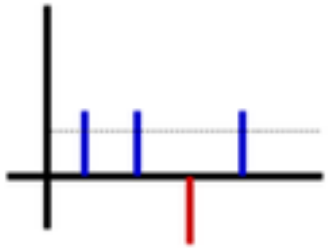
The Grover's data search algorithm – Graphical representation



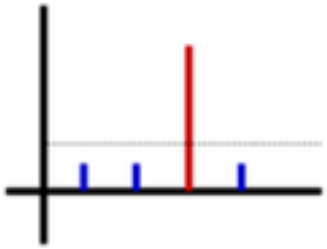
Original Amplitudes



Negate Amplitude



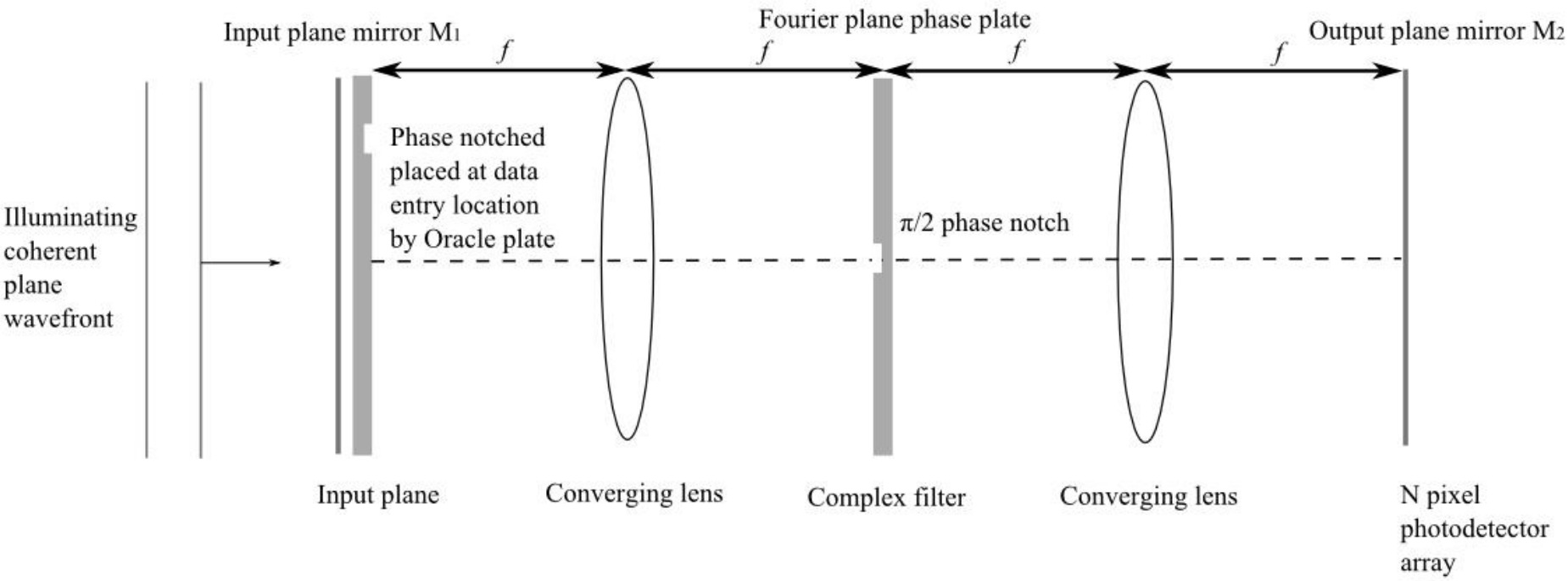
Average of all Amplitudes



Flip all Amplitudes around Avg

University of Sussex

Coherent optical implementation of the Grover algorithm using a Zernike phase contrast analogue

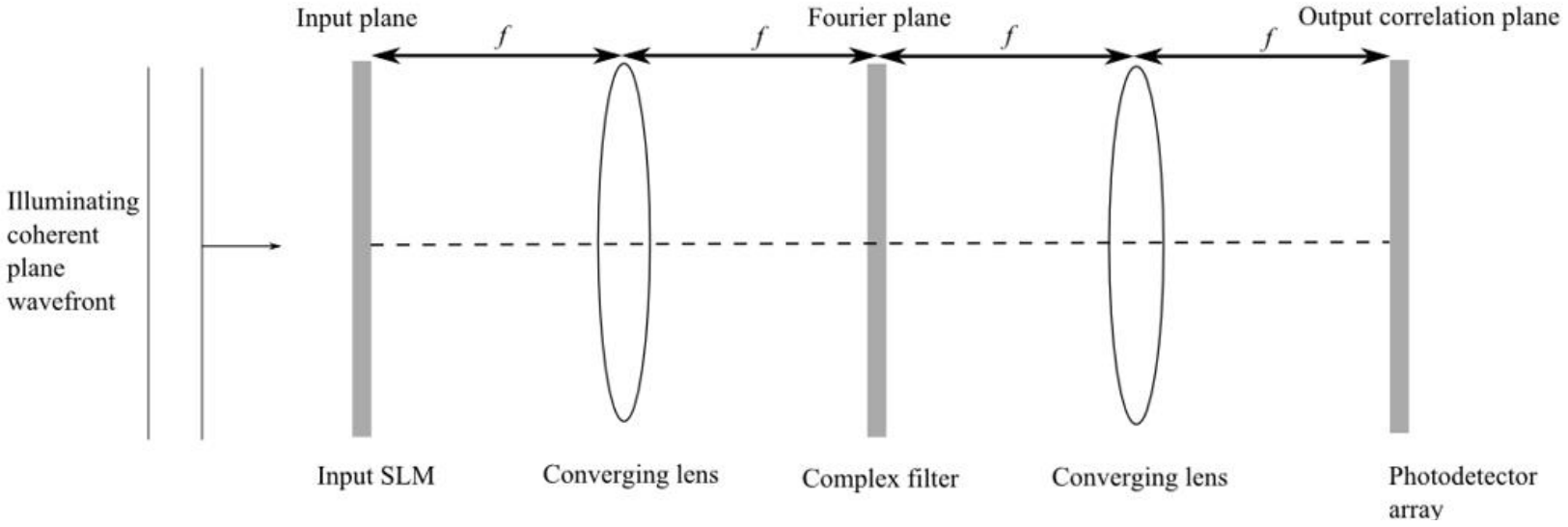


Bhattacharyia *et al*, *Phys. Rev. Lett.*, 2002

Hijmans *et al*. *JOSA B*, 2007

University of Sussex

Coherent optical implementation of the Grover algorithm using a matched filter – e.g. searching a phonebook



Input image

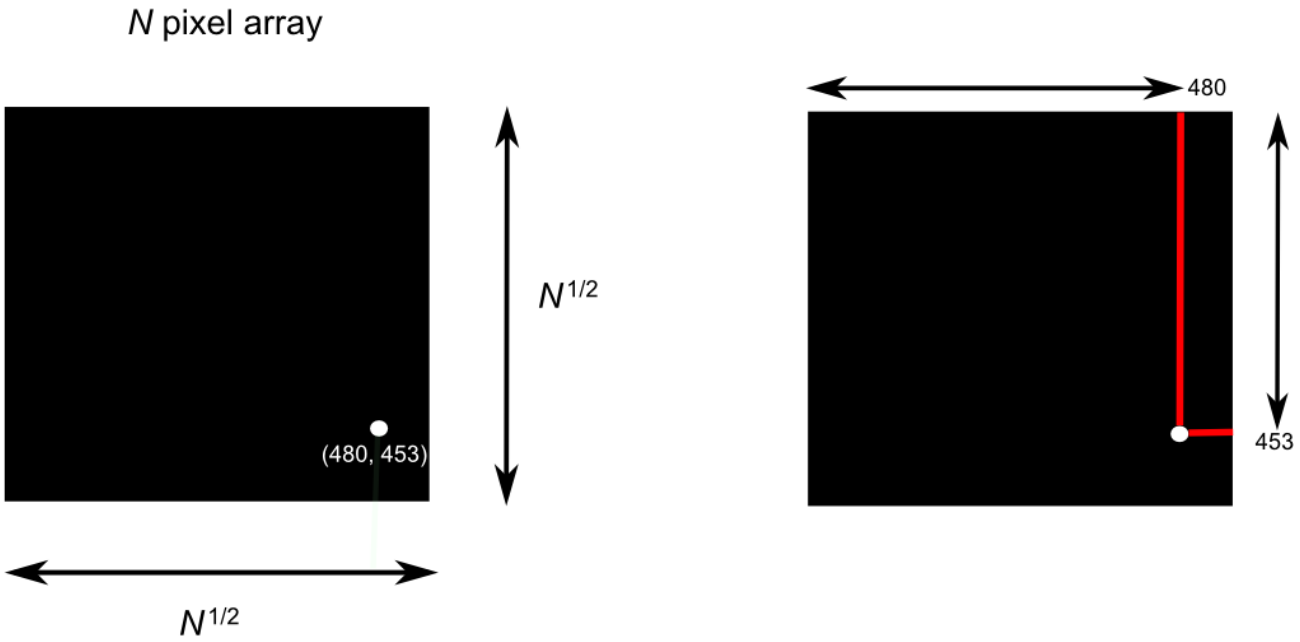
Reference image
(from which matched filter is made)

Correlation plane

University of Sussex

Location of correlation peak in $O\left(\sqrt{N}\right)$

- Direct search of *N* pixel array for the correlation peak requires O(*N*/2)
- To reduce this, project correlation peak onto *x* and *y* axes.
- The search then, on average, requires: $2 * \frac{N^{\frac{1}{2}}}{2}$ i.e. $O\left(\sqrt{N}\right)$ time



University of Sussex

Coherent optical implementation of the Discrete Fourier transform (DFT)

Forward DFT:

$$X(k) = \sum_{n=0}^{N-1} x(n) e^{-j\frac{2\pi nk}{N}}$$

$$k = 0,1,2,\ldots,N-1$$

Inverse DFT:

$$x(n) = \frac{1}{N} \sum_{k=0}^{N-1} X(k) e^{j\frac{2\pi nk}{N}}$$

$$n = 0,1,2,\ldots,N-1$$

Write:

$$e^{-j\frac{2\pi nk}{N}} = W_N^{nk}$$

N^2 complex multiplications for direct evaluation

University of Sussex

Coherent optical implementation of the Discrete Fourier transform (DFT)

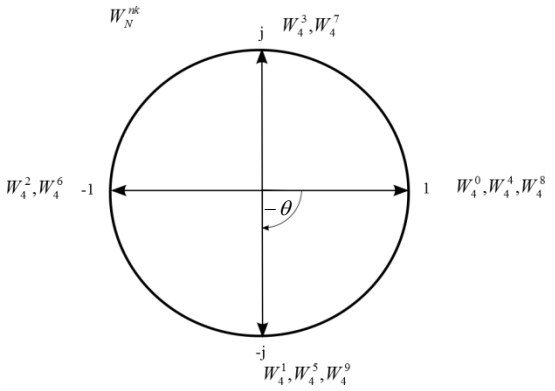
Can thus be written in matrix-vector form (for N=4):

$$\begin{bmatrix} X(0) \\ X(1) \\ X(2) \\ X(3) \end{bmatrix} = \begin{bmatrix} W_4^0 & W_4^0 & W_4^0 & W_4^0 \\ W_4^0 & W_4^1 & W_4^2 & W_4^3 \\ W_4^0 & W_4^2 & W_4^4 & W_4^6 \\ W_4^0 & W_4^3 & W_4^6 & W_4^9 \end{bmatrix} \begin{bmatrix} x(0) \\ x(1) \\ x(2) \\ x(3) \end{bmatrix}$$

where the matrix **W(*k*,*n*)** can be expressed in terms of phase only retardations:

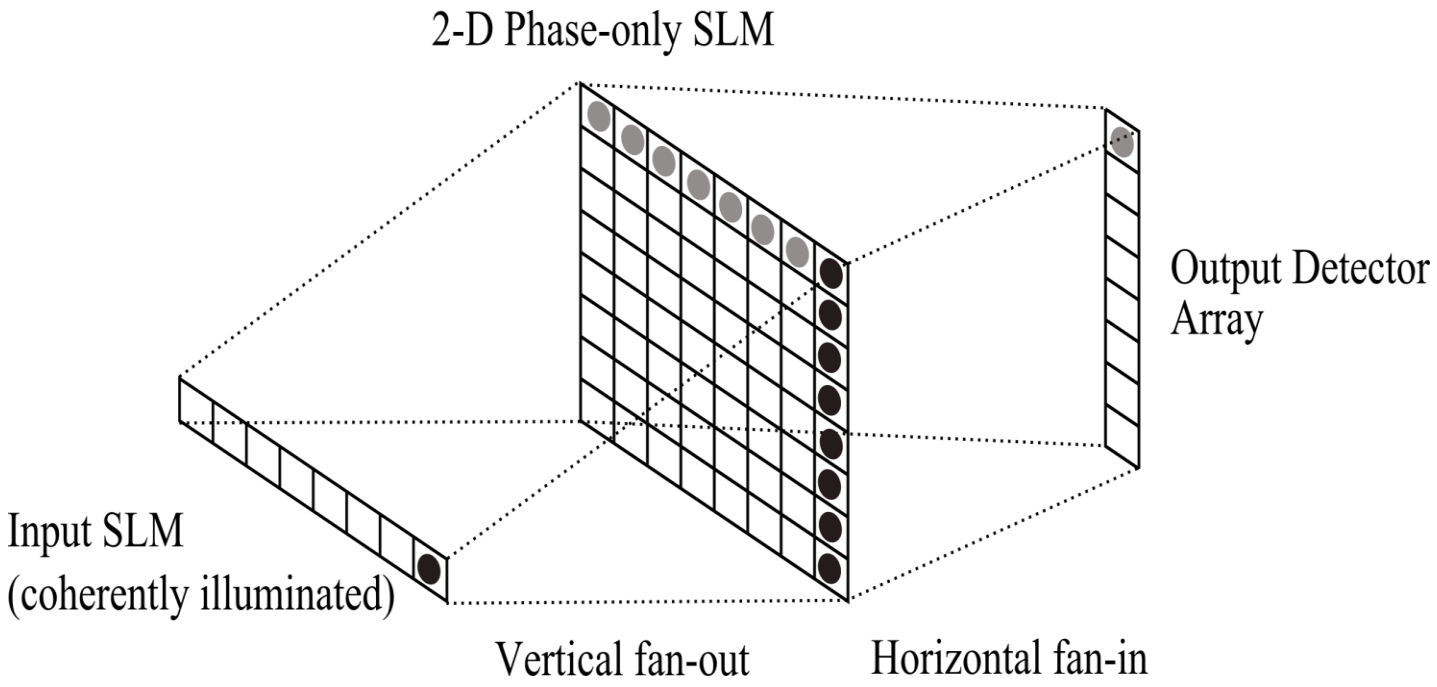
$$W(k,n) = \begin{bmatrix} e^{j0} & e^{j0} & e^{j0} & e^{j0} \\ e^{j0} & e^{-j\frac{\pi}{2}} & e^{-j\pi} & e^{-j\frac{3\pi}{2}} \\ e^{j0} & e^{-j\pi} & e^{-j0} & e^{-j\pi} \\ e^{j0} & e^{-j\frac{3\pi}{2}} & e^{-j\pi} & e^{-j\frac{\pi}{2}} \end{bmatrix}$$

Unit circle in the z-plane



University of Sussex

Coherent matrix-vector multiplier



Coherent matrix-vector multiplier for the calculation of the DFT

University of Sussex

DFT as a Unitary Operation

A unitary operation transforms one (complex) vector to another by multiplication with a matrix that has the property:

$$\mathbf{W}\mathbf{W}^{\Diamond} = \mathbf{I}$$

where the $\Diamond$ superscript indicates the conjugate transpose of the matrix.

Thus computation of the DFT can be implemented as a reversible, non-dissipative operation.

University of Sussex

Cooley-Tukey FFT decomposition of DFT (decimation in time); *N* a power of 2.

Half length DFTs of even and odd sequences:

$$X(k) = \sum_{n=0}^{\frac{N}{2}-1} x_1(n) W_{N/2}^{kn} + W_N^k \sum_{n=0}^{\frac{N}{2}-1} x_2(n) W_{N/2}^{kn}$$

which can be written for $k = 0,1,2,\ldots,\frac{N}{2}-1$:

$$X(k) = X_1(k) + W_N^k X_2(k)$$

by using the relation in W_N:

$$W_N^2 = \left(e^{-j\frac{2\pi}{N}} \right)^2 = e^{-j\frac{2\pi}{N/2}} = W_{N/2}$$

University of Sussex

FFT decomposition of DFT

Using the symmetry in W_N : $W_N^{k-\frac{N}{2}} = -W_N^k$

we also have:

$$X(k) = X_1(k - N/2) - W_N^k X_2(k - N/2)$$

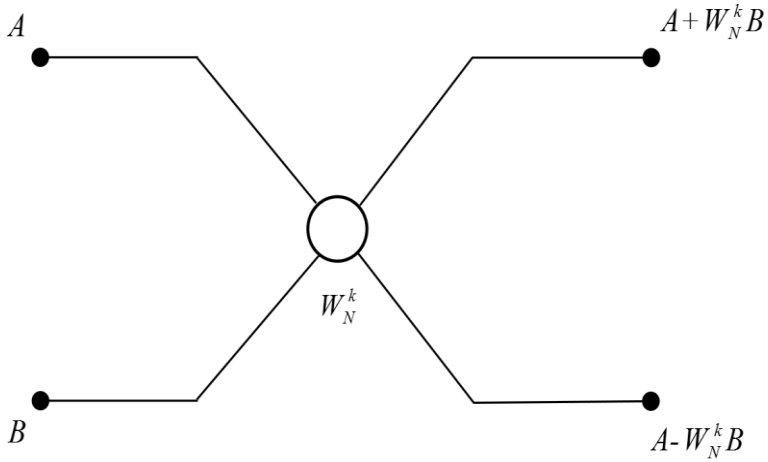
for values where: $\frac{N}{2} < k \leq N - 1$

Requires $N^2/2 + N/2$ complex multiplications

University of Sussex

FFT decomposition of DFT

Splitting into an even and odd sequence is repeated until there are *N*/2 2-point DFTs which can each be represented by the FFT Butterfly signal flow diagram:



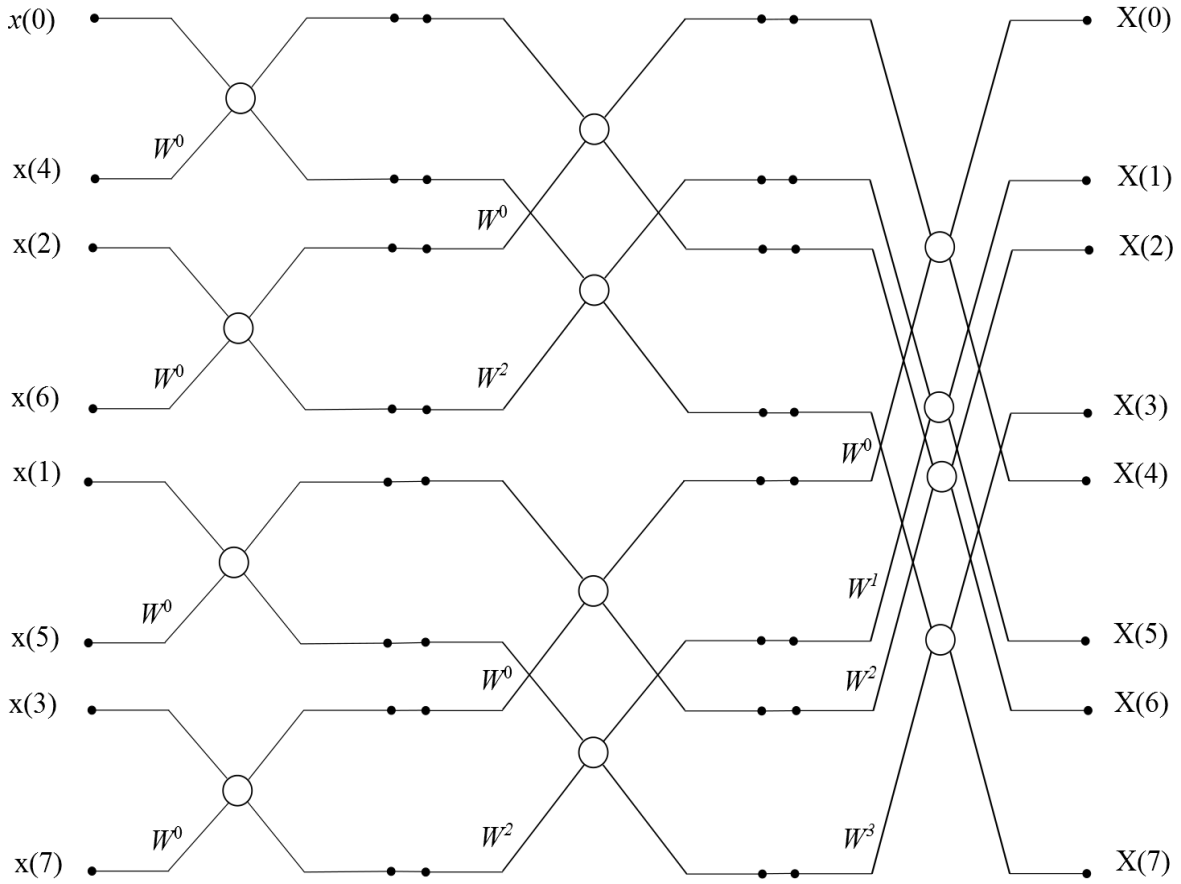
where for the 2-point transform W_N^k becomes W_N^0 i.e. unity.

Note that the computation involved in the Butterfly operation is Unitary.

University of Sussex

FFT decomposition of DFT (decimation in time)

Larger FFTs can then be built up from the basic Butterfly operations e.g. for an 8-point decimation in time FFT the signal flow graph is as shown below.



University of Sussex

Coherent optical implementation based on FFT signal flow diagram

Siegman (*Optics Letters*, 2001) suggested fibre optic implementation of FFT based DFT employing 50:50 FO couplers to implement the Butterfly operations

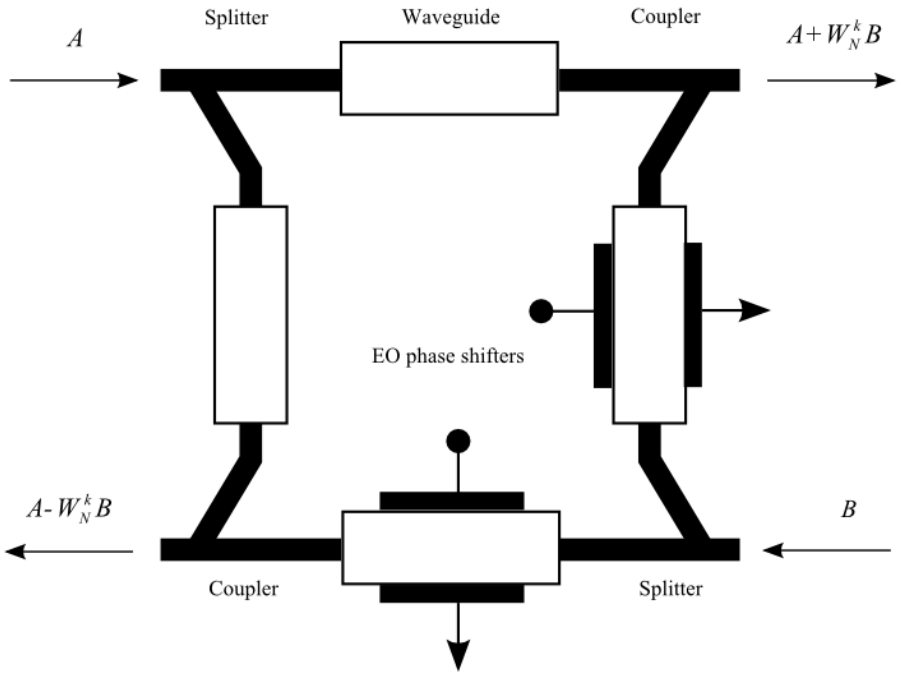
Another possibility is to employ slab waveguides integrated to a ‘hybrid device’ as used in fibre optics coherent detection systems

University of Sussex

Electro-optical implementation of the FFT Butterfly operation

Matrix-vector operation describing the hybrid:

$$\begin{bmatrix} E_{o1} \\ E_{o2} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & e^{-j\phi} \end{bmatrix} \begin{bmatrix} E_{i1} \\ E_{i2} \end{bmatrix}$$



Hybrid device for coherent addition with controlled relative phase delays

University of Sussex

The quantum Fourier transform (QFT)

The QFT acts on a wavefunction of, for example, four entangled ‘qubits’ (i.e. a one and zero superposition state at each bit location) described by the wavefunction or state vector:

$$|\psi\rangle = \sum_{n=0}^{N-1} x_n |n\rangle = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}$$

The wavefunction is the superposition of four qubits each weighted by a probability x_n representing the value of the input signal at that ‘qudit’ location:

$$|\psi\rangle = x_{00}|00\rangle + x_{01}|01\rangle + x_{10}|10\rangle + x_{11}|11\rangle$$

University of Sussex

The quantum Fourier transform (QFT)

The QFT of the state vector may then be computed:

$$\left|\Psi\right\rangle = \sum_{n=0}^{N-1} e^{-j\frac{2\pi nk}{N}} \left|\psi\right\rangle$$

which, since this is a unitary operation, maintains the wavefront superposition state but transforms it to the Fourier coefficients corresponding to the input wavefunction.

Thus we now have:

$$\left|\Psi\right\rangle = X_{00}\left|00\right\rangle + X_{01}\left|01\right\rangle + X_{10}\left|10\right\rangle + X_{11}\left|11\right\rangle$$

where the X_n are the complex coefficients corresponding to the complex Fourier components at that qudit location in the output array.

However, since they comprise the overall wavefunction, they will not be directly accessable to measurement. Rather the probability of detection, by a single photodetection event, will be given by $|\Psi|^2$.

University of Sussex

Similarities and differences of coherent optical FFT to the QFT

- If the input wavefunction is periodic, $|\Psi|^2$ will have a peak in its probability distribution at the output location corresponding to this.
- Thus repeated application of the QFT will yield more detection events at this location and hence allow determination of the periodicity, *r*.
- Thus the QFT is more powerful than the FFT in that it can process 2^N (binary) inputs in parallel with effectively the same complexity of hardware structure (and so is exponentially faster in computation).
- However, the FFT yields *N* complex frequency components at its output whereas the QFT produces a probability distribution only which collapses to a single photon detection event upon measurement.

University of Sussex

QFT implementation

An FFT-like decomposition of the QFT can be made using the Hadamard gate as the basic operation:

$$\mathbf{H} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

This arrangement will act on a single qubit state to give:

$$\mathbf{H}\left[x_0|0\rangle + x_1|1\rangle\right] = \frac{1}{\sqrt{2}}\left(x_0 + x_1\right)|0\rangle + \frac{1}{\sqrt{2}}\left(x_0 - x_1\right)|1\rangle$$

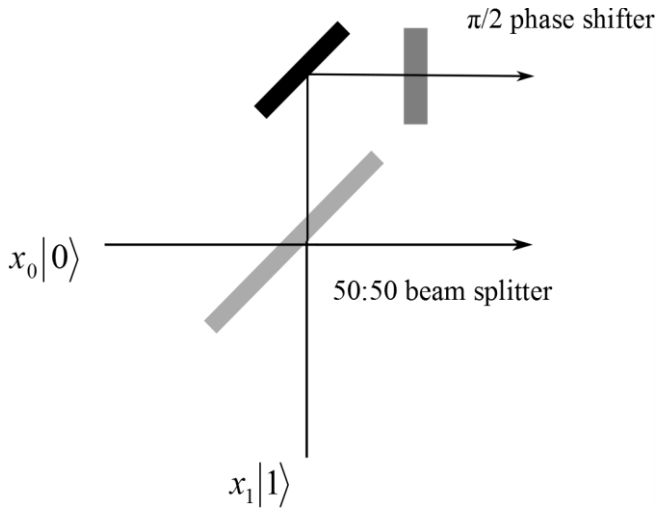
Thus it can be seen that the Hadamard transform performs a 2-point QFT by implementing the basic FFT building block of the Butterfly operation i.e. the subtraction and addition of the two input signals, albeit in a superposition state.

University of Sussex

QFT optical implementation

The basic operation comprising the Hadamard transform is optically implementable with a 50:50 beam splitter together with an additional $\pi/2$ phase shift in one of the beams as shown below (Barak and Ben-Aryeh, *JOSA* B, 2007).

This arrangement is also used in fibre optic communication coherent detection systems to realise a 180^0 hybrid.



Optical implementation of Hadamard gate

University of Sussex

QFT implementation

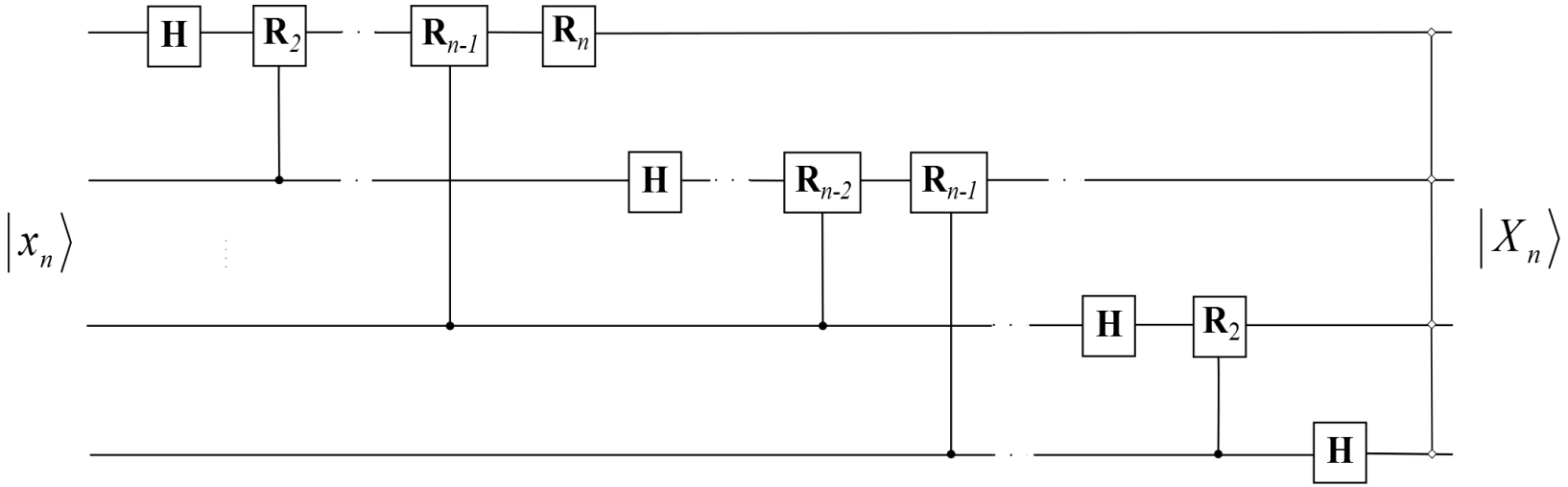
Larger count QTFs can be implemented by the same basic operation with the additional inclusion of controlled phase rotation gates described by matrices of the form:

$$R_n = \begin{bmatrix} 1 & 0 & 0 & . & 0 \\ 0 & 1 & 0 & . & 0 \\ 0 & 0 & 1 & . & 0 \\ . & . & . & . & . \\ 0 & 0 & 0 & . & e^{-j\frac{2\pi}{2^n}} \end{bmatrix}$$

University of Sussex

QFT implementation

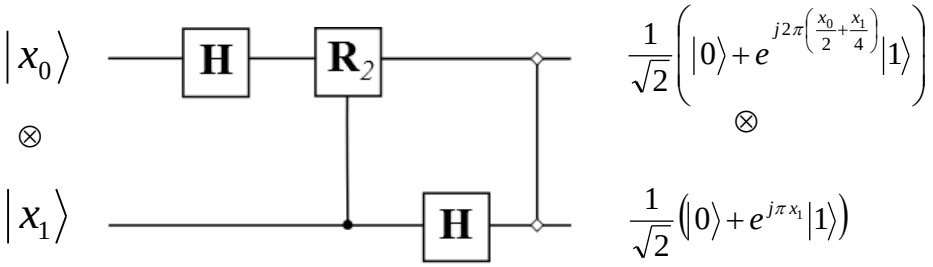
This allows the QFT structure for a *n*-qubit input to be represented compactly as shown below:

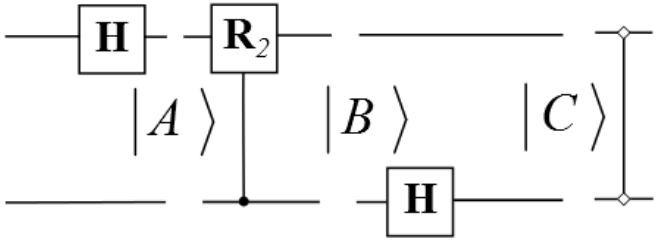


University of Sussex

Two Qubit QFT

The circuit to implement the two-qubit QFT is:





with $|A\rangle = U_1|x\rangle, |B\rangle = U_2|A\rangle, |C\rangle = U_3|B\rangle$ and $|X\rangle = U_4|C\rangle$

to, overall, yield: $F = U_4 U_3 U_2 U_1$

University of Sussex

Two Qubit QFT

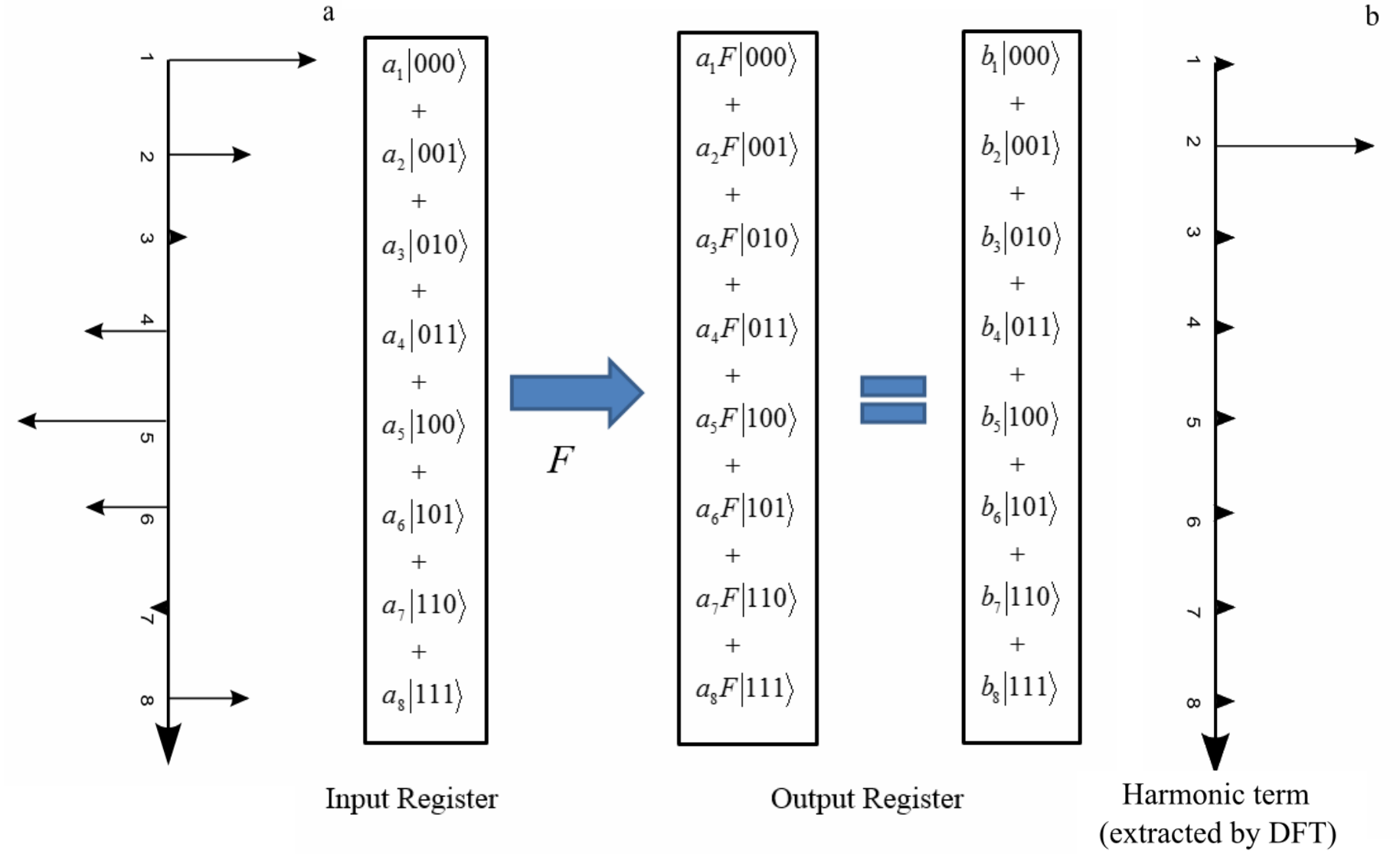
The unitary matrices for $n = 2$ are:

$$U_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \quad R_2 = U_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{-j\frac{\pi}{2}} \end{pmatrix} \quad U_3 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \quad U_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

to, overall, yield: $$F = U_4 U_3 U_2 U_1 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -j & -1 & j \\ 1 & -1 & 1 & -1 \\ 1 & j & -1 & -j \end{pmatrix}$$

University of Sussex

Unitary operation *F* on input register



University of Sussex

Shor's quantum factoring algorithm (1994) – factor very large numbers into prime factors, $N=p.q$

- Requires entanglement of bits in two quantum registers.
- Many superposition states are generated that the processor acts on with unitary operations in parallel, resulting in an exponential increase in processing power (SIMD operations).
- In order to factor a number N, a number q is chosen such that $N^2<q<2N^2$ to create a state in a quantum register:

$$|\psi_1\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a,0\rangle$$

- From which is computed:

$$|\psi_2\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, x^a \bmod N\rangle$$

University of Sussex

Shor's quantum factoring algorithm

- This operation results in a periodic function that can be related to the order, *r*, from which a factor of *N* can be derived.
- The QFT is used to perform a unitary transform of this state to:

$$\left|\psi_3\right\rangle = \frac{1}{\sqrt{q}} \sum_{m=0}^{q-1} \sum_{a=0}^{q-1} e^{-j\pi am/q} \left| m, x^a \bmod N \right\rangle$$

This results in a peak in the wavefunction which has a high probability of collapsing when a measurement is made, the location of which indicates the periodicity.

University of Sussex

Shor's quantum factoring algorithm

- Important result from Number Theory:

$$F(a) = x^a \bmod N$$

  is a periodic function

- Example: N = 15 and x =7 and we get the following:

$$7^0 \bmod(15) = 1$$
$$7^1 \bmod(15) = 7$$
$$7^2 \bmod(15) = 4$$
$$7^3 \bmod(15) = 13$$
$$7^4 \bmod(15) = 1$$
$$7^5 \bmod(15) = 7$$
$$7^6 \bmod(15) = 4$$
$$7^7 \bmod(15) = 13$$
$$\ldots.$$

University of Sussex

Shor's quantum factoring algorithm

- Thus we have order = 4
- Divide order by 2 and raise seed to this power:

$$7^{\frac{4}{2}} = 49$$

- Add or subtract 1 gives:

$$48 \quad \text{and} \quad 50$$

  - Greatest common divisor of 15 and 48 is: 3
  - Greatest common divisor of 15 and 50 is: 5
  - Thus 3 and 5 are factors of 15.
  - gcd can be determined for larger numbers by continued fraction expansion

University of Sussex

Shor's quantum factoring algorithm

- BUT : $N^2<q<2N^2$
- Typically N = 1024 bits so we have to perform

$$F(a) = x^a \bmod N$$

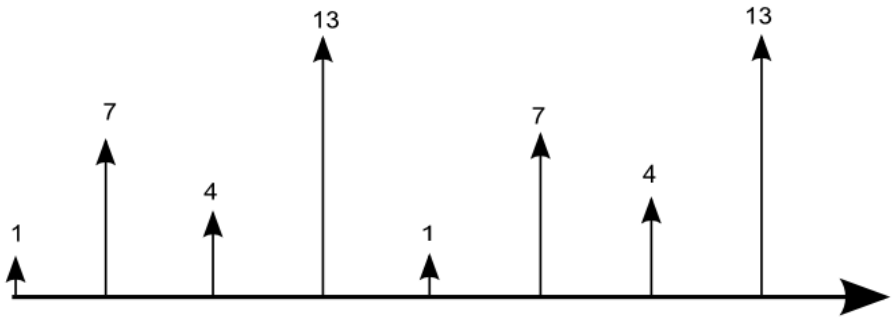
many times!

- But $F(a) = x^a \bmod N$ can be performed SIMD in a superposition state
- Measurement results in partial collapse of quantum register
- Associated wavefunction can undergo QFT without collapse

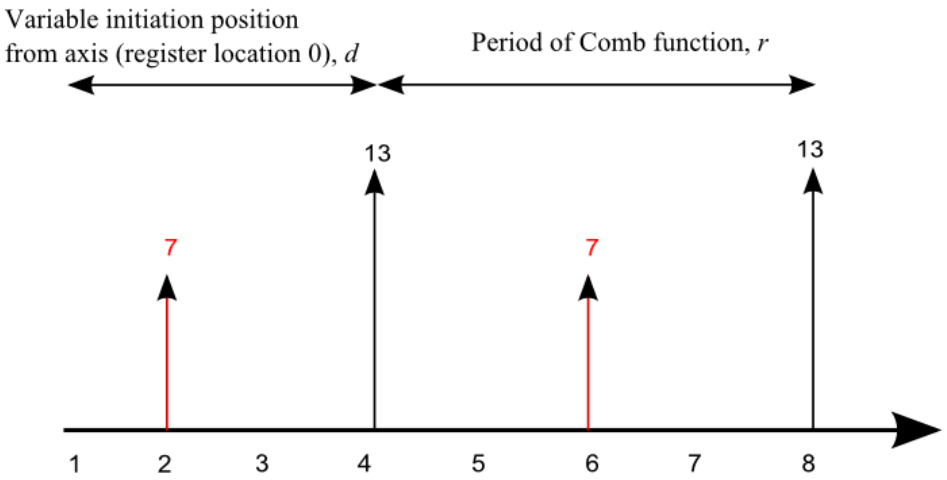
University of Sussex

Shor's quantum factoring algorithm

Register in superposition state



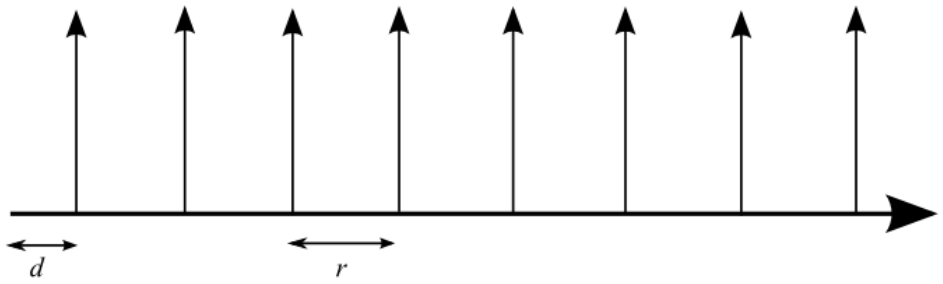
Register afer wavefunction collapse (only **one** impulse 'visible' after measurement)



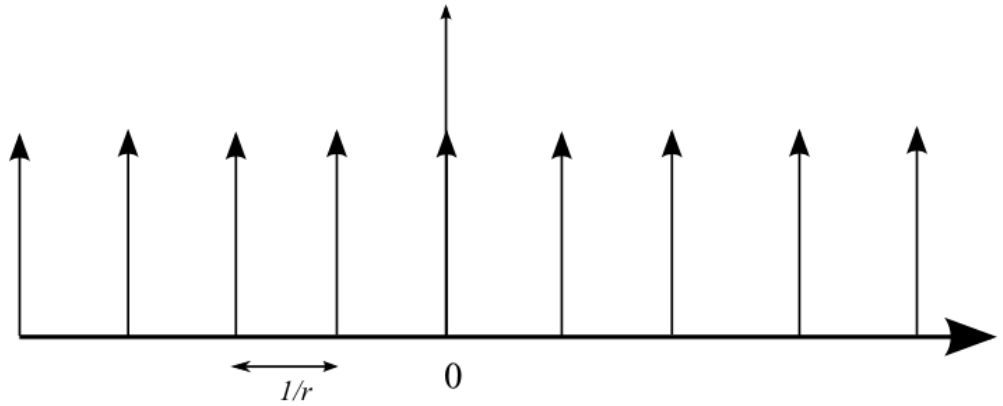
University of Sussex

Shor's quantum factoring algorithm

Second Register in superposition state



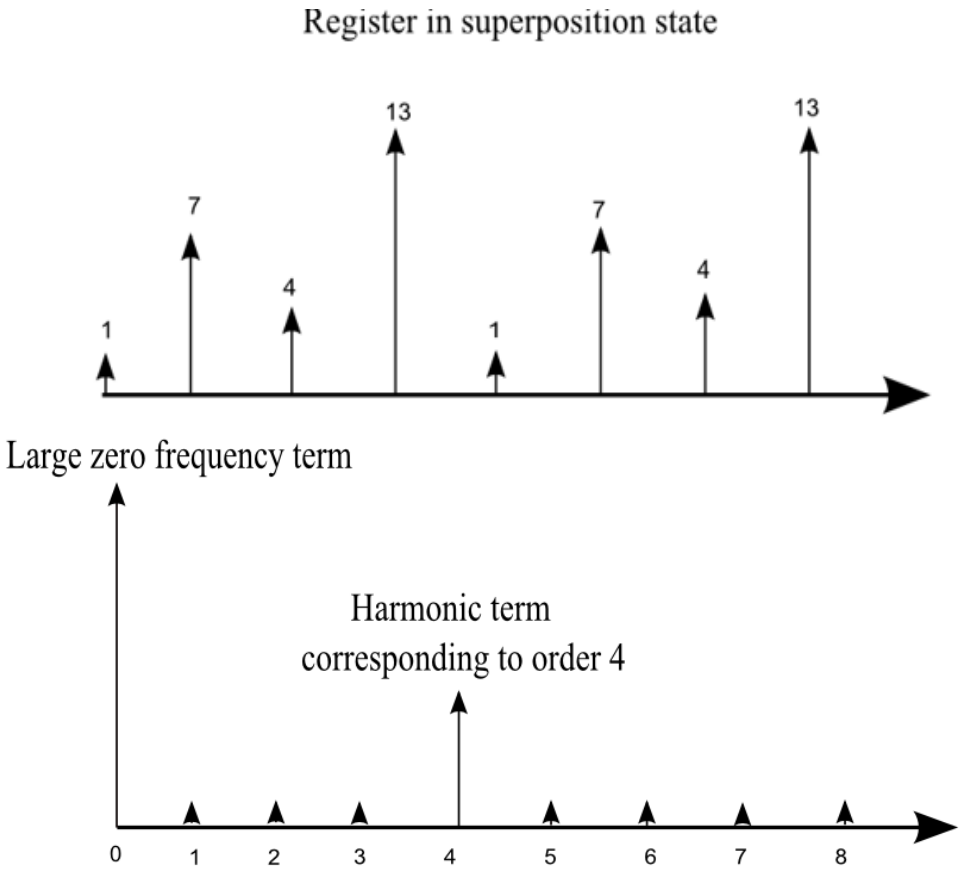
Second Register after QFT (only **one** impulse 'visible' after measurement)



University of Sussex

Possible simplifications of Shor's algorithm

- From single register, flip alternate register locations after calculation of $F(a)$ and then QFT directly



University of Sussex

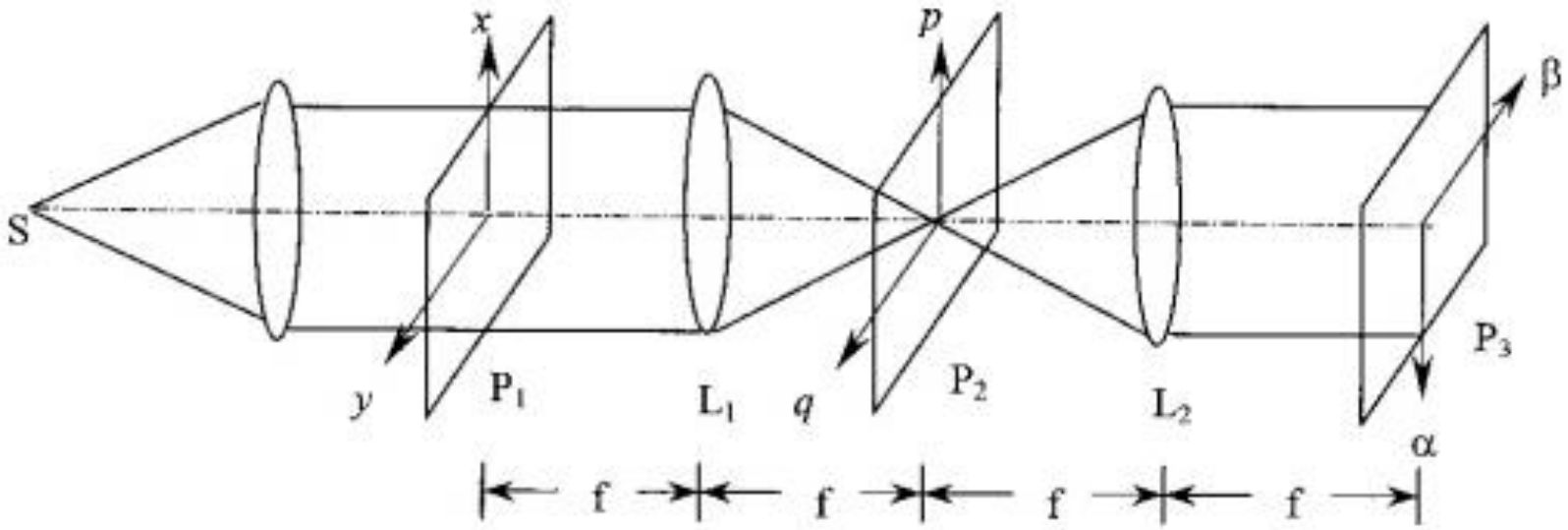
Possible simplifications of Shor's algorithm

- From single register with $F(a) = x^a \bmod N$
  flip alternate register locations and then QFT
- Employ a quantum Hadamard transform instead of QFT (eliminates requirement for R_n phase rotation gates)

University of Sussex

Coherent optical processor – 4-*f* correlator configuration

Spatial Light Modulator (SLM)



University of Sussex

SLM pixels placed in a superposition state

- SLM array of *N* discrete pixels
- Each pixel placed in a superposition state to form a qubit

Riedinger *et al*., "Non-classical correlations between single photons and phonons from a mechanical oscillator", *Letter to Nature*, doi:10.1038/nature16536, February 2016.

- Pixel qubit states entangled by addressing with an optical wavefunction to produce a superposition of the 2^N pixel states:

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x_n |n\rangle$$

using this as an "interaction free" measurement of the SLM qubits.

Elitzur and Vaidman, *Foundations of Physics*, 1993

Kwait *et al*, *Physical Review Letters*, 1995

University of Sussex

SLM pixels placed in a superposition state

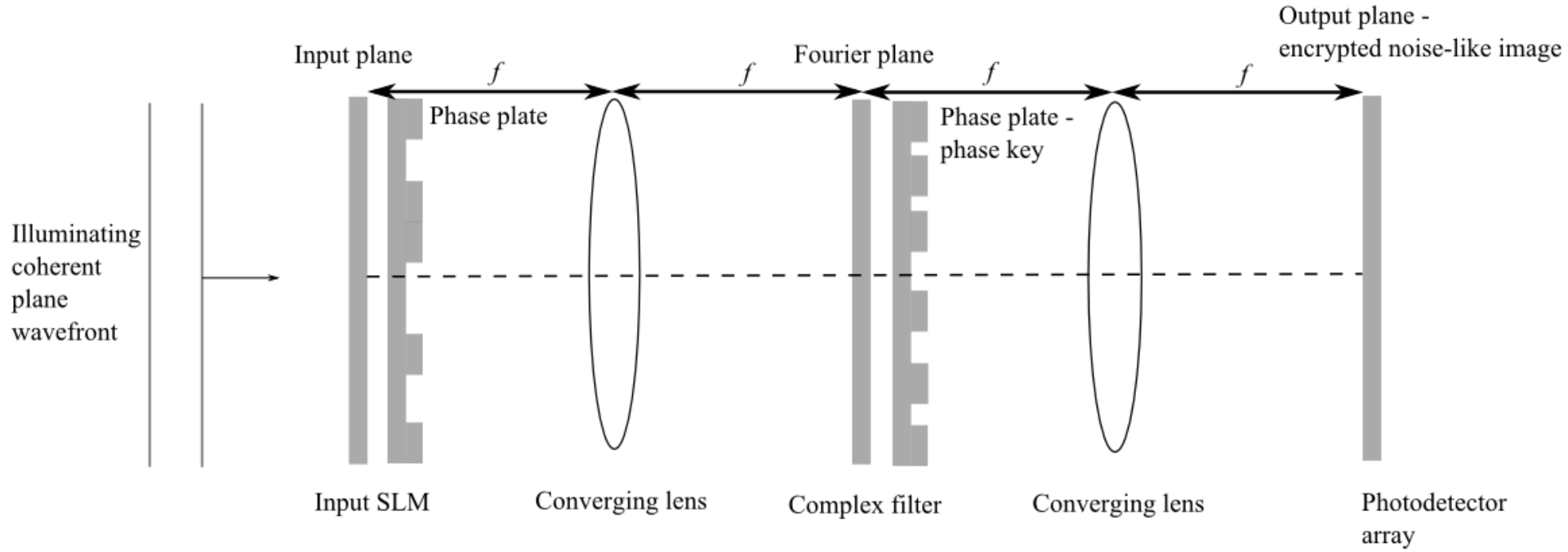
Kwiat P. G., Weinfurter H., Herzog T., Zeillinger A., Kasevich M. A., “Interaction-free measurements“, Phys. Rev. Lett., 74(24), 4763, (1995).

“If such systems (here discussing a physical system in a superposition state) are evaluated using interaction-free measurement schemes, then the two sub-systems – quantum object and the interrogating light – become entangled.

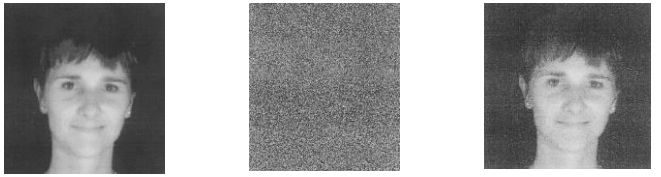
In fact, although we have not discussed it at all here, for sufficiently large *N* (number of measurement cycles), the interaction-free measurement methods even work for multi-photon states, even for dim classical pulses. Therefore, combining such an input with a quantum object, one is able to transfer quantum superposition of the latter into the former.”

University of Sussex

Example - optical image decryption

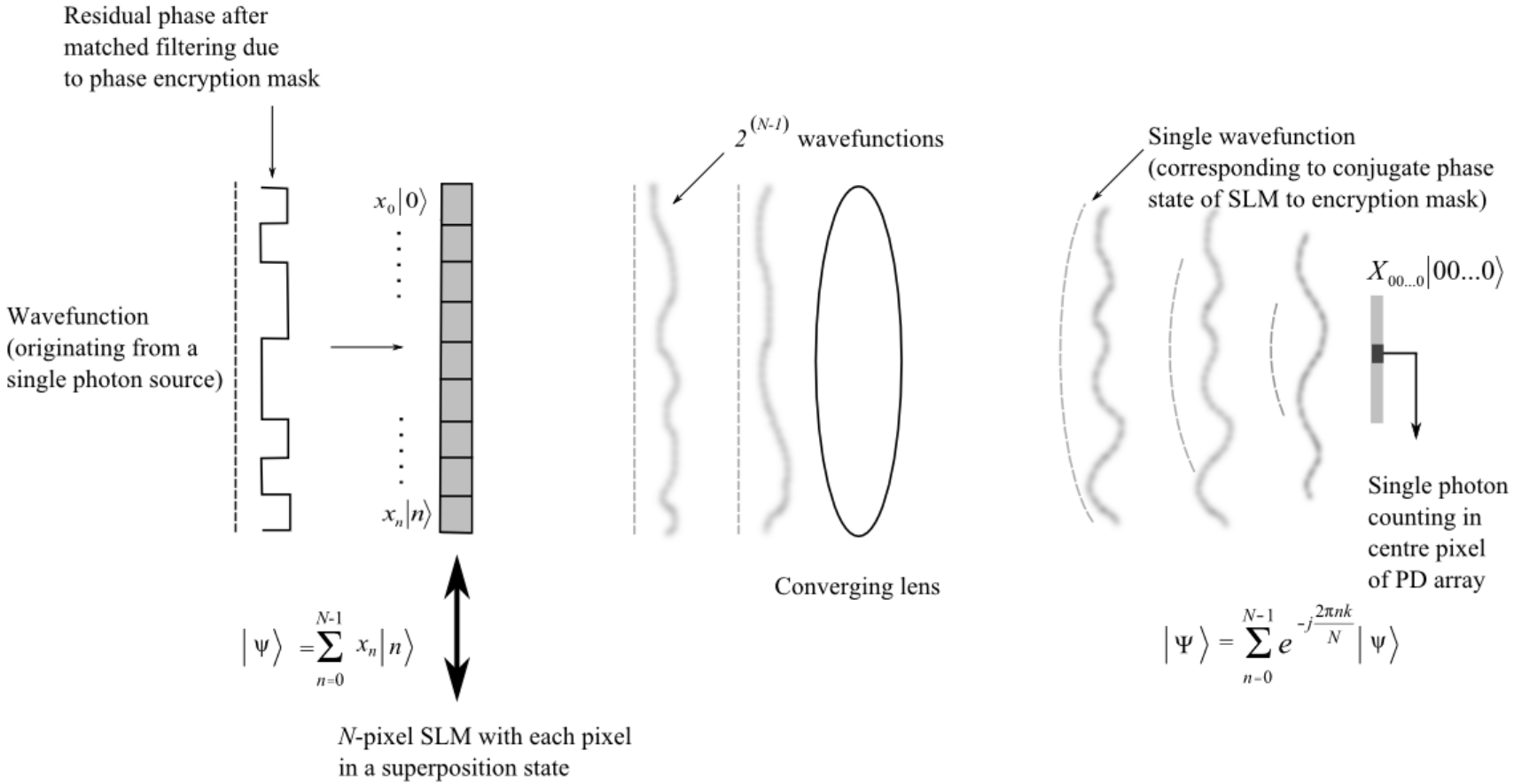


Refregier, Javidi, *Opt. Lett.* 1995



University of Sussex

Quantum optical processor for decryption task



A binary N-pixel 'quantum state' SLM will have 2^N combinations

University of Sussex

Conclusions

- Coherent optical implementation of the Grover algorithm is possible since it does not require entanglement of a quantum bit register.
- The Shor factorisation algorithm *does* require entanglement and so can only be implemented if this is arranged.
- If the pixels of an optically addressed SLM can each be placed in a binary superposition state and read out with an optical wavefront they will become entangled onto the wavefront.

University of Sussex

Conclusions

- If such an SLM can be incorporated into a coherent optical correlator 4-*f* optical configuration, the exponential increase in processing power typical of a quantum computation would be achievable.
- The implementation of quantum search-type algorithms may then be possible using this basic structure i.e. an analogue optical quantum computer could be constructed.
- This would be in contrast to the current approach of using discrete optical logic gates.
- For example, the required QFTs could be accomplished with a simple converging lens, rather than discrete QFTs employing individual Hadamard gates to implement an FFT-like decomposition.